NetworkCare
The knowledge behind the network

Lucent Technologies
Bell Labs Innovations

# Windows 2000 DNS Integration

*By Morgan Stern, Consultant, Global Engineering –*
*Lucent Technologies NetworkCare℠/Microsoft Alliance*

The purpose of this paper is to describe how Microsoft Windows 2000 systems utilize the Domain Name Service (DNS) to register and locate resources within a Windows 2000 network, and to discuss the issues related to integrating Windows 2000 in an existing DNS environment.

## Introduction

As the release of Windows 2000 draws closer, organizations are considering the benefits of migrating their existing networks to Windows 2000. Features such as Active Directory and Intellimirror, as well as improvements in scalability and stability, have addressed the concerns that many enterprises have had with Windows NT.

Taken as a collection of new technologies, Windows 2000 represents a major step in Microsoft's strategy of becoming the de facto OS for large enterprise environments. The most significant challenge for organizations will be to determine how best to deploy Windows 2000 technologies in their existing network environment while integrating these new features with existing production services.

One major new feature of Windows 2000 is the implementation of the Domain Name Service (DNS) as its primary name service. Windows 2000 domains by design are intrinsically linked to a DNS domain name. For example, windows.ins.com refers to a DNS name, but it also refers to a Windows 2000 domain name.

In this paper, we will discuss how Windows 2000 utilizes the DNS service for locating systems across a network. We'll also discuss some of the challenges associated with integrating a Windows 2000 name space with an existing DNS name space. Later, we'll discuss some interoperability issues and identify strategies for integrating Windows 2000 in an existing DNS environment.

This paper assumes a basic understanding of Windows 2000 as well as a more advanced understanding of the fundamentals of the Domain Name Service. For more information about DNS, read *DNS and Bind*, by Paul Albitz and Cricket Liu, published by O'Reilly.

## Naming Services - Locating Services Across the Network

In any network operating system environment, some service must provide the translation between user-friendly names (such as "Server1") and network addresses (such as 192.168.102.3). These translation services, also known as naming services, allow users to work with names that make sense to them, while computers can utilizes addresses more familiar to them.

In earlier versions of Windows NT, Microsoft relied upon a number of facilities to provide naming services: the NetBIOS naming standard, network browsing, and the Windows Internet Naming Service (WINS). Windows computers utilized these facilities both at bootup (to locate a domain controller for

authentication) and during normal operation (to locate servers to access client-server applications or to obtain file/print services).

While this collection of services provided adequate functionality for small and medium-sized organizations, they did not scale well in larger environments. For example, network browsing operations would inevitably become slow on a large network, frustrating users and administrators. Also, the WINS service (originally developed to enable NetBIOS name resolution across routed internetworks) became notorious for being difficult to manage and prone to database corruption.

Microsoft, in an attempt to mitigate existing shortcomings and to develop a system that would provide scalability for large enterprise environments, took a different approach with Windows 2000 naming services. The primary naming service for Windows 2000 will become the Domain Naming Service (DNS). (NetBIOS naming services will remain for compatibility with down-level clients in most environments. However, once an organization has migrated all systems to Windows 2000, NetBIOS support can be disabled.)

Microsoft's switch to DNS for Windows 2000 provides two benefits to implementers. First, by transitioning to an IETF standard protocol, Windows 2000 naming services should interoperate with standards-compliant DNS servers. Second, since DNS has been used for many years as the only naming service for the Internet, it is well understood as a protocol, and is considered to be a stable and mature technology. While both of these benefits are technically true, it will be critical for organizations to have a full understanding of how Windows 2000 utilizes DNS so that they can integrate Windows 2000 with their existing DNS infrastructure in a secure and scalable manner.

## How Windows 2000 Utilizes DNS

In a Windows 2000 environment, DNS becomes the facility for storage and retrieval of naming service information, both for: 1) network addresses of Windows 2000 systems, and 2) address and configuration information for Windows 2000 domains.

An example of Windows 2000/DNS interaction is summarized below.

Let's assume a small network of Windows 2000 systems – system A and system B.

Upon bootup, Windows 2000 system A registers its name and address in DNS. When system B needs to access system A, it retrieves system A's address from DNS and initiates a connection.

If system A is a Windows 2000 domain controller, it will also use DNS to store information about the Windows 2000 domain, so that system B can use DNS to locate the domain controller at authentication time.

Now let's continue with a more detailed explanation of these activities.

### *How Windows 2000 Systems Utilize DNS*

Each Windows 2000 system on a network will, by default, attempt to register itself in DNS through the use of an RFC 2136-compliant dynamic update. During the registration process, two types of resource records will be created: an address (A) resource record and a pointer (PTR) resource record.

A DNS address record contains two pieces of information, the hostname/domain of the system and its IP address. The host name for the Windows 2000 system corresponds to its workstation name, while the DNS domain suffix for the system is configurable via a client GUI, the registry, or by group policy object (GPO). (The combination of system host name and domain suffix is typically referred to as the fully qualified domain name, or FQDN.)

Most organizations will likely utilize the DNS domain suffix that corresponds to the Windows 2000/Active Directory domain in which the system is a member, while other organizations may wish to use a DNS domain suffix that would place host records in an existing corporate DNS namespace. We will discuss issues related to these alternatives later.

Under normal operating conditions, a Windows 2000 system will create the address record upon bootup, and will refresh the record every 24 hours. When the system is shut down, it will delete the address record. In order for the system to perform these operations, the Windows 2000 system must first locate the primary server for the appropriate DNS zone (as identified in the start of authority (SOA) record for the zone) and the zone must be configured to support and accept dynamic DNS updates.

The second type of DNS resource record, a pointer (PTR) record, is utilized for reverse DNS lookups – for times when the IP address of a system is known and the DNS name needs to be determined. (Some organizations require reverse lookups for security and auditing purposes.)

On each Windows 2000 system, the service that is responsible for managing DNS record updates is the DHCP client service, which runs regardless of whether the system is configured to receive an IP address via DHCP or by static assignment.

Resource record registration occurs in one of four ways:

1. If the system is configured with a static IP address, the DHCP client service will contact the primary DNS server directly to register both the address (A) and pointer (PTR) records.
2. If the system is configured to receive an IP address from a DHCP server, the DHCP client service will negotiate responsibility for updating DNS records with the DHCP server. By default, Windows 2000 systems will attempt to register their own address records while relying on a DHCP server to perform the registration of the pointer (PTR) resource record for reverse lookup functionality.
3. If the DHCP server does not support dynamic updates of the PTR record, the Windows 2000 system will update the PTR record itself.
4. In some cases, the DHCP server may be configured to ignore the client and generate both the A record update and the PTR record update itself.

All interactions between the Windows 2000 DHCP client service and the DHCP server are performed according to the specifications outlined in an RFC draft document (http://www.ietf.org/internet-drafts/draft-ietf-dhc-dhcp-dns-10.txt). Negotiation between the client and DHCP server is achieved through the use of DHCP Option 81. Using option 81, the DHCP client can inform the server of the system's fully qualified domain name. In addition, either the client or the server can assume responsibility for creating the dynamic update for the DNS address record.

### *How Windows 2000 Domain Controllers Utilize DNS*

While all systems follow the same process for generating dynamic updates of DNS address and pointer records, Windows 2000 domain controllers interact with DNS in one additional, but very significant, way.

When a Windows 2000 domain controller boots up, it not only initiates the registration of the A and PTR records, but also creates a series of DNS server (SRV) records that correspond to the Windows 2000 domain itself. These SRV records are used by Windows 2000 clients to locate domain information, and are organized according to criteria such as the site name or server type (i.e., global catalog, domain controller, kerberos authentication server). By creating a series of SRV records instead of one single entry, Windows 2000 clients can locate the most appropriate controller based upon a number of criteria, such as physical proximity.

When a domain controller creates an SRV record, the record is placed in the Windows 2000 DNS domain. For example, with a Windows 2000 domain name of ins.com, the SRV record names would similar to the example shown below:

*_ldap._tcp.ins.com*

SRV records contain seven pieces of information: service, protocol, domain name, priority, weight, port number, and target host. The table below describes each of the elements in more detail.

| Element | Function |
|---|---|
| Service | Refers to the type of service provided. Typical values might include _ldap, _kerberos, _kpassword, _gc |
| Protocol | Refers to the transport protocol used by the service, either _tcp or _udp |
| Domain | The domain name refers to the DNS domain name for the Windows 2000 domain. |
| Priority | Priority provides a function similar to the preference value in an MX DNS record. If multiple SRV records exist for the same service, clients will always attempt to access the host with the lowest priority value. |
| Weight | The weight value fulfills a similar role to priority, but is intended for load balancing. If multiple records have an equal priority value, the chance of a record being chosen will be proportional to the weight value. |
| Port number | Refers to the port number for the service (i.e., LDAP utilizes port 389). |
| Target host | Identifies the DNS name for the server that offers the service (a corresponding DNS address record must exist for the host). |

Using the earlier example, the full SRV record might contain the following information:

- Service = ldap
- Protocol = tcp
- Domain name = ins.com
- Priority = 0
- Weight = 100
- Port = 389
- Target host = server11.ins.com

In addition to the SRV records, each domain controller also registers additional address (A) DNS records to simplify the domain controller location process for Windows 2000 clients.

### How Windows 2000 Systems Locate the Domain Controller

When a Windows 2000 system boots up, the Netlogon service initiates the process of locating the Active Directory domain. This process collects information from the registry, including the name of the Active Directory domain for which the system is a member. It then initiates a DNS lookup to locate SRV records for that domain. Once it locates the appropriate SRV records, the system will initiate an LDAP query to the domain controller to initiate the authentication process.

Windows 2000 systems can select domain controllers based upon different criteria. For example, if the system is located in a site called NYC, it can select a domain controller in NYC by locating the SRV record *_kerberos._tcp.NYC._sites.dc._msdcs.ins.com.* This mechanism enables clients to reduce WAN-related authentication traffic by always connecting to the closest domain controller.

## DNS Name Space Integration

Now that we've discussed how Windows 2000 systems interact with DNS, the challenge for many organizations will to be to integrate their Active Directory domains within an existing DNS name space.

As discussed earlier, Windows 2000 domains are intrinsically linked to a DNS domain name. If an organization does not have a pre-existing DNS name space, it can implement a new DNS infrastructure to manage its Windows 2000/DNS domain naming system. If, however, the organization has an existing DNS name space, it will be forced integrate its existing DNS domains with the new Windows 2000/DNS domains.

Let's consider two scenarios to illustrate this issue – the first scenario is relatively simple, while the second is less straightforward. Throughout these examples, we will assume that each organization maintains separate DNS systems for their internal systems and their Internet-connected systems (Web server, Mail server, etc.) for security purposes.

### *Scenario 1 – Single Domain In Pre-Existing DNS Name Space*

In this scenario, our example organization is a medium-sized company called Medsize Inc., with 5,000 users on their network. They have a single pre-existing internal corporate DNS domain, medsize.com, that contains approximately 150 resource records for their mainframe system, some UNIX hosts, a few intranet web servers, and some NT servers. Their Windows NT domain model is a single domain called, appropriately enough, MEDSIZE.

The IT group decides to migrate the entire Windows NT infrastructure to Windows 2000. One key decision they need to make is the new name for the Windows 2000 domain. The simplest option is to name the Windows 2000 domain medsize.com, the same as the corporate DNS name. In this case, no changes need to be made to the production DNS name space because Windows 2000 will utilize the existing domain name. From a DNS name space perspective, this approach makes sense. However, the IT group may need to address some interoperability issues, depending on what type (and version) of DNS server they currently use. We'll discuss interoperability issues later.

### *Scenario 2 – Multiple Domains In Pre-Existing DNS Name Space*

In this scenario, our example organization is a much larger company called Bigsize Inc. The Bigsize network is large, containing 90,000 users spread across 500 offices in 30 countries. There are five business units within Bigsize: Sales, Engineering, Marketing, Manufacturing, and Research. Most offices contain users from 3 or more business units.

The Bigsize internal DNS name space reflects Bigsize's geographically-dispersed environment, with the use of regional domains and country-based subdomains. For example, all hostnames for systems in the United States exist within a DNS domain called *us.Americas.bigsize.com*, while hostnames for systems in Japan exist in jp.Asia.bigsize.com. Due to security issues, every computer on the network has a DNS host record. The entire DNS name space contains more than 94,000 resource records.

The Bigsize Windows NT environment includes approximately 1,000 servers. The domain model contains five master domains (each business unit has its own account domain) and 100 resource domains. Each of the five business units has an administrative team that is responsible for resources and accounts owned by the business unit. Corporate standards are developed by an IT committee comprised of IT leaders from each of the business units.

At their quarterly meeting, the IT committee decides to migrate the entire Windows NT environment to Windows 2000 to simplify the domain model and reduce the overall cost of administration. To begin the process, the committee nominates a team to develop recommendations for the new Windows 2000 domain model, including a strategy for integrating the new model with the existing DNS name space.

As you can imagine, the Windows 2000 committee has some considerable issues to resolve. Their first decision (for security and administrative reasons) is that each of the five account domains will remain, while all resources in the resource domains will be migrated into the new Windows 2000 domains and placed in organizational units.

At this point, the good news is that they are planning to move from 105 Windows NT domains down to 5 Windows 2000 domains. The bad news is that the five new Windows 2000 domains, which are still based upon business units, do not correspond in any way to the existing production DNS name space, which is based on geographical location.

After considering their options, the Windows 2000 committee decides to extend their DNS name space to include five new subdomains, each named after one of the business units: sales.bigsize.com, engineering.bigsize.com, marketing.bigsize.com, and so on. These new domains will exist alongside the existing geographically-organized DNS domains. DNS resource records for the Windows 2000 domain controllers (including address and SRV records) will exist in the new domains, while host records for workstations will remain in their original DNS domains.

### *Lessons Learned*

These scenarios demonstrate two possible approaches to integrating Windows 2000 domains into an existing DNS name space. In the first scenario, the integration was straightforward and required no changes to the existing DNS name space. In the second scenario, some substantial changes were required to accommodate the new Windows 2000 DNS domains.

The most important lesson from scenario 2 is that a Windows 2000 domain naming system does not have to be shoehorned into an existing DNS name space, nor does an existing DNS name space have to be eliminated to make room to deploy Windows 2000 domains. By paying close attention to administrative and business requirements from both a DNS and a Windows 2000 perspective, designers can create a model that accommodates both systems, while leveraging an existing infrastructure.

## Interoperability Considerations

Since many organizations have made significant investments to deploy a DNS infrastructure throughout their production environment, a large percentage of Windows 2000 deployments will involve integration with existing DNS services. It is important to mention a number of issues related to Windows 2000 and DNS interoperability.

### *Minimum Requirements*

In discussing how Windows 2000 systems utilize DNS, we covered two functions that are critical for proper Windows 2000 functioning: dynamic DNS updates and support for SRV records. While both functions are supported by the DNS server that ships with Windows 2000, not all non-Microsoft DNS servers support them. Organizations which intend to utilize their existing DNS server infrastructure for Windows 2000 will need to confirm that their servers support both RFC 2052 (SRV records) and RFC 2136 (dynamic DNS).

For UNIX-based DNS servers, BIND version 8.1.2 and higher support both DDNS and SRV records.

### *Other Considerations*

While support for RFCs 2052 and 2136 are an absolute minimum for a DNS server to interoperate with Windows 2000, there are some other factors to be considered.

#### Secure Updates

While Dynamic DNS eliminates a considerable amount of DNS administration by allowing workstations to manage their own DNS resource records, it also introduces some potential security issues.

In current implementations of BIND, Dynamic DNS can be enabled at the domain level or at the server level. Once enabled, any network client can send updates to the DNS server, including clients that have been configured (either unintentionally or maliciously) with an incorrect name. For example, a system that was mistakenly named ‘www’ could send a dynamic update to overwrite a legitimate DNS entry for a company’s DNS server.

In anticipation of this type of misuse of dynamic DNS, a secure version of Dynamic DNS (DNSSEC) was specified in RFC 2137. However, while BIND version 8.1 was the first to implement RFC 2136 dynamic update, it was not until version 8.2 that any support for DNSSEC was provided. (BIND 8.1.x does, however, provide the ability to control dynamic updates via IP address.)

However, because RFC 2137 was not complete when Windows 2000 was being designed, Microsoft implemented a different secure update system based upon IETF draft documents.

It is important to note that Microsoft’s implementation of secure DNS update does not interoperate with DNS servers that support RFC 2137, so currently there is no mechanism to enforce secure DNS updates between Windows 2000 systems and a BIND DNS server.

It is also important to recognize that Windows 2000 DNS only provides secure updates when the DNS zones are configured as *Active Directory Integrated* zones. If a Windows 2000 DNS server contains zones that are configured as *Standard Primary* zones, no security is provided.

The lack of secure updates between Windows 2000 and BIND will likely cause problems for a number of organizations. We’ll discuss some options for these organizations in a section below entitled “DNS Implementation Strategies.”

#### Character Restrictions

Historically, DNS systems administrators have followed a host naming convention that was defined in RFC 921, wherein the only characters considered valid were alpha, numeric, or the minus (-) sign. Some DNS servers, including some versions of BIND, would enforce these naming conventions by discarding any host names that did not adhere to the convention.

In an effort to maintain standardization and to avoid compatibility problems, many DNS administrators have become sensitive to the types of characters that can legitimately be used in DNS. As you may have noticed from our earlier discussion about SRV records, Windows 2000 utilizes the underscore (_) character in every SRV record. This has caused concern among many DNS administrators, and will continue to be a topic for debate into the future.

Organizations that have an existing non-Microsoft DNS infrastructure in place will need to address two points to overcome possible objections:

1. Underscores are now considered to be part of the valid character set for DNS names, per RFC 2181, which states that a DNS name can contain any binary string, including characters such as the underscore.
2. Some versions of BIND must be configured NOT to discard DNS names that contain underscores. Administrators can accomplish this by using the 'check-names' directive in either the boot file or a specific zone file for the DNS server. By default, a primary DNS server will discard invalid DNS names. By including the directive 'check-names ignore' or 'check-names warn', the DNS server will not discard invalid names, but will instead accept them without warning, or will accept the name but generate an warning message to the system log.

## DHCP Issues

Most large organizations recognize the benefits of implementing the Dynamic Host Configuration Protocol (DHCP) on their network to provide automatic assignment of IP addresses to network-attached computers. Use of DHCP has become widespread, so it is important to understand issues related to integrating DHCP and Windows 2000.

As we discussed earlier, the DHCP client service on a Windows 2000 system is responsible for managing how the DNS records (both the address record and the PTR) for that system are registered.

When the system is configured to obtain an IP address from a DHCP server, the DHCP client service will attempt to negotiate with the DHCP server to determine whether the client service or the DHCP server will perform the dynamic DNS updates for the resource records. The default method of operation is for the DHCP client service to register the address record, while the DHCP server assumes responsibility for registering the pointer (PTR) record for reverse lookups.

The key interoperability issue during this transaction relates to the mechanism that the DHCP client service uses to inform the DHCP server of the host name of the system, DHCP option 81. A DHCP server must support DHCP option 81 in order to identify the hostname of the Windows 2000 system correctly. As of the time of writing this paper, only the DHCP server included with Windows 2000 provides support for DHCP option 81. However, most vendors of DHCP software have committed to providing option 81 support in upcoming releases of their products, either as new versions or as service releases.

## DNS Implementation Strategies

Now that we have discussed how Windows 2000 utilizes DNS and have identified the interoperability issues between Windows 2000 and non-Microsoft DNS servers, we'll conclude by describing three strategies for implementing a Windows 2000 integrated DNS system. We'll review each strategy by asking four questions:

1. How well does it leverage the existing DNS infrastructure?
2. How much security does it provide?
3. What are the compatibility issues?
4. What type of an organization might want to consider this option?

### *Strategy One – 100% Windows DNS*

The first option is to install a new DNS infrastructure using the DNS server software that is included with Windows 2000. This is the strategy that is most highly recommended by Microsoft, because it eliminates the possibility of interoperability issues.

#### How well does it leverage the existing DNS infrastructure?

This strategy does not make any attempt to leverage any existing investment in a DNS infrastructure. In fact, if an organization has existing DNS servers, they would have to completely replace them with Windows 2000-based DNS servers. Many organizations will not consider this an acceptable option, and will instead opt to preserve their original investment by choosing to implement either strategy two or strategy three.

#### How much security does it provide?

From a security standpoint, this strategy will provide the highest level of security, assuming the Windows 2000 zones are configured as *Active Directory Integrated* zones. If this is the case, the secure update mechanism will prohibit any attempts by non-authenticated systems to register DNS resource records via DDNS.

#### What are the compatibility issues?

This strategy avoids any compatibility issues by utilizing Microsoft as the single vendor for all components.

#### What type of an organization might want to consider this option?

This option may be appealing to those organizations that currently do not have any DNS servers on their network, or to those organizations who have a minimal existing DNS architecture but are extremely concerned with security and are unwilling to consider any other options.

### *Strategy Two – 100% BIND DNS*

The second approach is to integrate an organization's entire existing DNS infrastructure with Windows 2000 and to avoid using Microsoft DNS completely.

This option may be appealing to organizations that have made significant investments in a DNS infrastructure, but there are some issues they will need to resolve before implementing this strategy.

### How well does it leverage the existing DNS infrastructure?

This strategy helps an organization preserve its initial investments in DNS by fully leveraging the existing architecture. For some larger organizations that have purchased expensive DNS management systems, this will be a major factor.

### How much security does it provide?

The downside of this strategy is that it provides very little (almost non-existent) security. As we discussed earlier, the secure updates functionality provided by Windows 2000 is not compatible with the DNSSEC specification, so the only mechanism for controlling security on dynamic updates is to specify IP addresses of systems that are authorized to perform updates. This type of an arrangement is not scalable enough for most organizations.

### What are the compatibility issues?

While the DNSSEC compatibility issue is important from a security standpoint, there are other more essential issues that must be considered.

In order for any non-Microsoft DNS server to integrate with Windows 2000 systems, it must support RFCs 2136 and 2052 for dynamic DNS and SRV records. In addition, the DNS configuration files may need to have the 'check-names' directive included so that they do not reject host names that contain characters such as the underscore (_).

### What type of an organization might want to consider this option?

The types of organizations that might consider this option are those who have already invested in large scale DNS architecture (that meets their current needs outside of Windows 2000) and are willing to assume the risks associated with the lack of secure dynamic DNS updates.

## *Strategy Three – Hybrid DNS*

The third strategy incorporates the benefits of strategies one and two, while attempting to mitigate some of the limitations.

Organizations that choose to utilize strategy three will retain their existing DNS infrastructure and will implement Windows 2000-based DNS only when absolutely necessary. This type of an implementation may take one of two forms:

1. DNS records for all Windows 2000 domain controllers, servers, and workstations are contained in DNS domains that correspond to the Windows 2000 domains.
2. DNS records for Windows 2000 domain controllers exist in the DNS/Windows 2000 domains, while DNS records for all other Windows 2000 systems (servers and workstations) are contained in their original DNS domains.

### How well does it leverage the existing DNS infrastructure?

This strategy leverages the existing DNS infrastructure well. Organizations can continue to use their existing systems and tools to manage the bulk of their DNS infrastructure, thereby retaining their original investment.

However, it is important to note one factor. If an organization chooses to place DNS records for all Windows 2000 systems (domain controllers, servers, workstations) in the DNS/Active Directory domain,

and if a high percentage of corporate systems will be migrated to Windows 2000, the majority of the DNS resource records will ultimately end up on a Windows-2000 DNS server. In this scenario, as systems are upgraded, DNS records will migrate from their original location in the existing DNS space to the new Windows 2000 domains. The alternative is to keep DNS records in their original locations and either utilize a DHCP server to manage dynamic updates or shut off dynamic updates altogether and use static DNS records for servers or other systems that absolutely require a DNS record.

### How much security does it provide?

This strategy provides security where it is most important. By utilizing a Windows 2000 DNS server for the DNS/Active Directory domains, administrators can enable secure updates for the SRV records associated with domain controllers. This will prevent the ability for unauthorized systems to impersonate domain controllers or to assume control of a domain.

If the organization chooses to keep DNS records for non-DC servers and workstations in their original BIND-hosted domains, they can avoid security problems by disabling dynamic updates on the BIND server and by using static DNS addresses for servers and other essential systems.

### What are the compatibility issues?

This strategy has some of the same compatibility issues as strategy two, but they become less critical since a Windows 2000 DNS server is managing all domain and domain controller-related DNS activity.

This strategy may work with any version of BIND, depending upon which approach the organization chooses to implement. If they choose to not utilize dynamic updates for any of their Windows 2000 workstations, they can use virtually any version of BIND. However, if they do wish to use dynamic updates for their non-domain controller systems, they will need to confirm that the version of BIND on their DNS servers supports dynamic updates, and that DDNS has been enabled for the appropriate DNS zones. They may also need to utilize the ‘check-names’ directive if the host names of their Windows 2000 systems utilize any (previously) invalid characters.

### What type of an organization might want to consider this option?

Most large organizations will want to consider this option, since it allows them to leverage their existing DNS infrastructure, while also providing a higher level of security for the DNS updates for the essential Windows 2000 servers.

## Conclusion

While Windows 2000 addresses the shortcomings of Microsoft’s previous Windows naming services, it also introduces an additional level of complexity. Organizations that plan to implement Windows 2000 will have some complex decisions in order to successfully integrate it with their existing DNS infrastructures. Those who will be successful are the ones who carefully balance the impact of a Windows 2000/DNS integration while paying close attention to interoperability and security issues

For further information, see NetworkCare's website at http://www.lucent-networkcare.com or call 1-888-767-2988 in the U.S. or 1-727-217-2303 outside the U.S.